AP 1A - Threat of or Actual Contamination to Water System

POSSIBLE STAGE

AP Summary:	This Action Plan applies to the intentional introduction of a contaminant into the water system. The contaminant could be introduced at any point within the system, including raw water, treatment facilities, distribution system including distribution pipes, finished water storage, or pump stations. The adversary may or may not give notice of the contaminant or provide the location. Contamination may have actually occurred or it may be a hoax.	
Initiation and Notification:	1. Initiate this AP if any of the following has occurred: Security Breach (including, for example): • Unsecured Doors • Open Hatches • Unlocked/Forced Gates • Fence Break • Trampled Grass/Tracks • Alarm Triggered Witness Account (including, for example): • Suspicious Activity • Trespassing • Breaking and Entering • Tampering with Equipment or Property Direct Notification by Perpetrator (including, for example): • Verbal Threat • Threat in Writing Notification by Law Enforcement (including, for example): • Suspicious Activity • Threat made to Water System Notification by News Media (including, for example): • Threat Delivered to News Media • Media Discovers Threat Unusual Water Quality Parameters (including, for example): • Changes in pH, Fluoride residual or turbidity	*Use this AP if you receive any incident warning (see types of warnings to left) indicating possible contamination of your water system* *If you have evidence that corroborates the warning, or if collective information indicates that contamination is likely,* ***GO TO AP 1B – CREDIBLE STAGE.*** *If there is confirmed evidence and/or definitive information that the water system has been contaminated.* ***GO TO AP 1C – CONFIRMED STAGE.***

AP 1A - Threat of or Actual Contamination to Water System POSSIBLE STAGE		
	• Unexpected monitoring or sampling results • Strange odor, color or appearance Customer Complaints (including, for example unexplained or unusually high complaints of): • Odor • Color or Appearance • Taste Public Health Notification (including, for example): • Victims in Emergency Rooms and/or Clinics • High Incidence of Similar Health Complaints in one Local Area	
Initiation and Notification:	2. Notify GM or designee and appropriate Division Supervisor immediately upon discovery of any of the above Threat Warnings.	*The individual who first notices or receives the threat warning should contact the GM immediately by whatever means of communication may be available.*
Equipment Identified:	Equipment Location	*This equipment is available to assist in the execution of this AP.*
Specific Activities:		
I. Assess the Problem	A. Complete the following **Threat Warning Report Forms** according to the type of Threat Warning received. (Appendix G of ERP). • **Security Incident Report Form (G-10 & G-11)** • **Witness Account Report Form (G-21 & G-22)** • **Phone Threat Report Form** ***(to be filled out during actual phone call) (G-6 & G-7)*** • **Written Threat Report Form (G-1 & G-2)** • **Water Quality / Consumer Complaint Report Form (G-20)** • **Public Health Information Report Form (G-8 & G-9)**	*Threat Warning Report Forms help document, organize and summarize information about a security incident. The individual who discovers the incident warning, the GM, or another designated individual may complete the form. Only the form that corresponds to the type of threat warning needs to be completed. Completion of the form should not distract emergency responders from more urgent matters.* *Threat Evaluation Worksheets help organize information*

AP 1A - Threat of or Actual Contamination to Water System POSSIBLE STAGE		
	B. Complete **Threat Evaluation Worksheet (Appendix G, Pgs. G-17 to G-19 of the ERP).** C. Evaluate **Threat Evaluation Worksheet**, and determine if threat is Possible. If YES, perform Response Steps 1 – 8 below. If NO, 1. Return to normal operations. 2. Document and record the threat for future reference.	*about a threat warning that will be used during the Threat Evaluation Process. The individual responsible for conducting the Threat Evaluation (e.g., the GM) should complete this worksheet.*
II. Isolate and Fix the Problem	1. Notify local law enforcement. 2. Notify State Drinking Water Agency. 3. Do not disturb site if location could be possible crime scene. Consult **Maintaining Crime Scene Integrity Form in Appendix G, Page G-5.** 4. Alert staff and emergency response personnel about threat. 5. Consider containment / isolation, elevating chlorination, and/or discharge of suspect water. 6. Evaluate spread of suspect water and potential impact on public health.	*Notification phone numbers can be obtained from the Organization Contact List in Appendix D, Table D-2 as well as from Section 6.1DSRSD Chain of Command of the Emergency Response Plan, (ERP).* *The immediate operational response actions are primarily intended to limit exposure of customers to potentially contaminated water.*
III. Monitoring	7. Initiate Site Characterization Activities: • Define the investigation site. • Designate site characterization team members. • Conduct preliminary assessment of potential site hazards. • Approach site and conduct field safety screening to detect any hazards to the characterization team. • Search for physical evidence (discarded containers, etc.). • Investigate records from CCTV cameras. • Look for environmental indicators (dead animals or fish, dead vegetation, unusual	*Site Characterization is intended to gather critical information to support the 'credible' stage of threat evaluation.* *If signs of a hazard are evident during the site approach, the team should halt their approach and immediately inform the GM of their findings. The site may then be turned over to the HAZMAT Team.* *The GM may determine the threat is credible based preliminary information before the site characterization has*

AP 1A - Threat of or Actual Contamination to Water System POSSIBLE STAGE		
	odors or residues). • Perform rapid field testing of the water. • Collect water samples according to sampling plan.	*been completed.*
IV. Recovery and Return to Safety	8. Determine if threat is credible. If YES, initiate AP 1B. If NO, • Return to normal operations. • Store water samples for as long as determined by the DHS.	*You should determine whether or not the threat is 'credible' within 2 to 8 hours (preferably within 2 hours) from the time the threat is deemed 'possible', depending on the effectiveness of the containment strategy.* *If the threat is not deemed 'credible', the samples obtained during site characterization should be stored in case the situation changes and analysis is determined to be necessary.*
V. Report of Findings	9. File incident reports.	*The Utility GM should file an internal report for the Utility's files, and also provide information as requested to Local Law Enforcement.*
VI. AP-1A Revision Dates		

AP 1B - Threat of or Actual Contamination to Water System

CREDIBLE STAGE

AP Summary:	This Action Plan applies to the intentional introduction of a contaminant into the water system. The contaminant could be introduced at any point within the system, including raw water, treatment facilities, distribution system including distribution pipes, finished water storage, or pump stations. The adversary may or may not give notice, identify the contaminant, or provide the location. Contamination may have actually occurred or it may be a hoax.	
Initiation and Notification:	A. Initiate this AP if there is credible evidence that the water system has been contaminated: • Additional information collected during the investigation corroborates the threat warning. • Collective information indicates that contamination is likely. • Signs of contamination are observed during site characterization. • Additional water quality data shows unusual trends that are consistent with the initial data and corroborate the threat. • A pattern of customer complaints emerges. • Previous threats and incidents corroborate the current threat. B. Notify GM or designee immediately upon discovery of credible evidence of threat (if not already notified). C. Initiate ERP. D. Initiate partial or full activation of the Emergency Operations Center (EOC). Perform internal and external notifications according to ERP.	*If there is confirmed evidence and/or definitive information that the water system has been contaminated,* ***GO TO AP 1C – CONFIRMED STAGE.*** *The individual who first notices or receives the credible evidence should contact the GM immediately by whatever means of communication may be available.* *The GM will decide whether to initiate the ERP on a partial or full basis. The GM will also decide when and to what extent to activate the EOC.* *Notification phone numbers can be obtained from the Organization Contact List in Appendix D, Table D-2 as well as from Section 6.1DSRSD Chain of Command of the Emergency Response Plan, (ERP).* *The PIO is the only one authorized to make notifications to outside agencies.*
Equipment Identified:	Equipment	*This equipment is available to assist in the execution of this AP.*

AP 1B - Threat of or Actual Contamination to Water System CREDIBLE STAGE		
	Location	
Specific Activities:		
I. Assess the Problem	1. Assess results of previous sample analysis. 2. Perform additional site characterization at primary sites as needed. 3. Perform site characterization at any new investigation sites.	
II. Isolate and Fix the Problem	4. Perform actions to estimate the contaminated area and predict movement of contamination. 5. Take actions to isolate portions of system containing suspect water. *See* ERP Appendix C for System Shut Down Plan beginning at page C-1. 6. Issue "Boil Water", "Do not Drink", or "Do not Use" orders and Press Releases as appropriate. See Appendix F of ERP for **Press Release Forms.** Initiate **Alternate Water Supply Plan** to provide alternate water supply for customers. Discussion at Section 3.1.3. At present, there is no alternate source for fire protection.	*The contaminated area can be estimated using hydraulic models, consumer complaints, public health agency reports, water quality data, or other available information. The estimate may define additional locations where site characterization should be performed*
III. Monitoring	7. Continue to monitor water quality in suspect parts of system by manual sampling, rapid field testing, or automated means.	
IV. Recovery and Return to Safety	8. Determine if threat is Confirmed. If YES, Initiate AP 1C. If NO, • Verify that water is safe. • Notify public that water is safe. • Notify outside agencies that water is safe. • Return to normal operations. • Store water samples for as long as determined by the DHS.	*It may take several days to collect sufficient evidence to confirm a contamination incident, depending on the type of information used for confirmation. (Some microbiological analytical procedures may take several days.)* *If the threat is not deemed 'confirmed', the samples obtained during site characterization should be stored in case the situation changes and an analysis is*

AP 1B - Threat of or Actual Contamination to Water System CREDIBLE STAGE		
		determined to be necessary.
V. Report of Findings	E. File incident reports.	*The Utility GM should file an internal report for the Utility's files, and also provide information as requested to Local Law Enforcement and other outside agencies.*
VI. AP-1B Revision Dates		

This page has been intentionally left blank.

AP 1C - Contamination to Water System

CONFIRMED STAGE

AP Summary:	This Action Plan applies to the intentional introduction of a contaminant into the water system. The contaminant could be introduced at any point within the system, including raw water, treatment facilities, distribution system including distribution pipes, finished water storage, or pump stations. The adversary may or may not give notice, identify the contaminant, or provide the location. Contamination may have actually occurred or it may be a hoax.	
Initiation and Notification:	A. Initiate this AP if there is confirmed evidence that the water system has been contaminated: 3. There is **analytical confirmation** of the presence of one or more contaminants in the water system. 4. The **preponderance of the evidence** confirms that a contamination incident has occurred. • There is a security breach with obvious signs of contamination along with unusual water quality and consumer complaints in the vicinity of the security breach. • Additional findings (laboratory analysis, field observations) of continued site characterization activities add to other credible evidence of contamination. • There is information from public health officials, area hospitals, or 911 call centers indicating a problem with the water supply. • Law enforcement agencies have discovered crucial evidence or apprehended a suspect that helps confirm that the water has been contaminated. • Specific information on a number of potential contaminants can be used in conjunction with other available	*If there is <u>no</u> confirmed evidence and no definitive information that the water system has been threatened or contaminated,* ***GO TO AP 1B – CREDIBLE STAGE.*** *It may take several days to collect sufficient evidence to confirm a contamination incident, and the required time will depend on the type of information used for confirmation (some microbial analytical procedures may take several days).*

AP 1C - Contamination to Water System CONFIRMED STAGE		
	information to narrow down the number of contaminant candidates.	
Initiation and Notification:	B. Notify GM or designee immediately upon discovery of confirmed evidence of contamination (if not already notified). C. Initiate full ERP activation. D. Initiate full activation of Emergency Operations Center (EOC). E. Engage other organization as needed (drinking water primacy agency, public health agency, response agencies, law enforcement). F. Perform internal and external notifications according to ERP.	*The individual who first becomes aware of the confirmed evidence should contact the GM immediately by whatever means of communication may be available.* *The GM will decide whether to initiate the ERP on a partial or full basis. The GM will also decide when and to what extent to activate the EOC.* *Notification phone numbers can be obtained from the Organization Contact List in the Appendices as well as from Section XX of the ERP.* *The PIO should make the notifications to the outside agencies.*
Equipment Identified:	**Equipment** **Location**	*This equipment is available to assist in the execution of this AP.*
Specific Activities:		
I. Assess the Problem	1. Assess results of previous sample analysis and attempt to identify the contaminant. 2. Confirm the identity of the contaminant.	*Effective implementation of response actions depends on positive identification of the contaminant and knowledge of contaminant properties, including public health protection strategies and selection of treatment technologies.*
I. Assess the Problem	3. Perform a full characterization of the contaminated area, including contaminant properties, contaminant concentration profiles, and characteristics of the impacted area. 4. Evaluate the likely direction and extent of future movement of the contaminant within the distribution system. 5. Evaluate all available information about	*If information from site characterization activities indicates that the contaminant impacts water quality in a certain manner (i.e., consumes free Fluoride or imparts a certain odor to the water), the contaminant specific information may facilitate tentative identification of a contaminant and determine the analytical approach that should be used to positively identify the specific contaminant. Sources of contaminant information include:*

AP 1C - Contamination to Water System CONFIRMED STAGE		
	the contamination incident.	*http://www.bt.cdc.gov/agent/agentlistchem.asp* *http://www.cdc.gov/atsdr/index.html* *http://www.waterisac.org/* *EPA Water Contaminant Information Tool (WCIT) – under development*
II. Isolate and Fix the Problem	6. Take actions to isolate portions of system containing suspect water. See ERP Appendix C beginning at Page C-1 for **System Shut Down Plan.** 7. Shut down system if obvious or confirmed contamination warrants. 8. Issue "Boil Water", "Do not Drink", or "Do not Use" orders and Press Releases as appropriate. See Appendix F of ERP for **Press Release Forms.** 9. Initiate **Alternate Water Supply Plan** to provide alternate water supply for customers. Discussion at Section 3.1.3. At present, there is no alternate source for fire protection. 10. Revise public health response measures and public notifications as necessary.	*The contaminated area can be estimated using hydraulic modes, consumer complaints, public health agency reports, water quality data, or other available information. The estimate may define additional locations where site characterization should be performed.*
III. Monitoring	11. Continue sampling and analysis to monitor the status and extent of the contamination, and to verify that containment strategies are working.	
IV. Recovery and Return to Safety	12. Consult with appropriate officials to develop a Remediation and Recovery Plan. a. Evaluate options for treating contaminated water and rehabilitating system components. b. Select treatment and rehabilitation	*Remediation and recovery activities will likely be planned and implemented by a number of agencies. The first step of the process is to establish the roles and responsibilities of each organization* *The samples obtained during site characterization and monitoring should be stored(as determined by the DHS) in case the situation changes and further analysis is determined to be necessary.*

	technology/approach. c. Develop strategy for disposal of contaminated residuals. d. Develop sampling and analysis plan to verify remediation. e. Develop communications and public relations plan. 13. Implement Remediation and Recovery Plan. a. Verify that water is safe by performing additional sampling and analysis to confirm the progress of system treatment and remediation. b. Notify public that water is safe. c. Notify outside agencies that water is safe. d. Return to normal operations. e. Store water samples for as long as determined by the DHS.	
V. Report of Findings	G. File incident reports with internal and external agencies as required.	*The Utility GM should file an internal report for the Utility's files, and also provide information as requested to outside agencies.*
VI. AP-1C Revision Dates		

AP 2 - Structural Damage from Explosive Device

AP Summary:	This Action Plan applies to an incident where intentional structural damage has occurred to the water system as a result of an explosive device. The assumed intent of the explosion is to disrupt normal system operations any point within the system, including raw water, treatment, finished water storage, or the distribution network.	
Initiation and Notification:	A. Initiate this AP if it appears that an explosive device has caused damage, or has the potential to cause damage to one or more components of the water system. The event will begin with an "incident discovery" which may come to DSRSD by one (or more) of the following: • Security Systems • Employee Discovery • Witness Account of Explosion • Notification By Adversary • Notification by Fire Department • Notification By Law Enforcement • Notification By News Media B. Call 911 and notify GM or designee, District Engineer and appropriate Division Supervisor upon discovery of the explosion. The GM should then notify others as appropriate. Examples include: a. Local Fire Department b. Local Police Department c. FBI d. ATF C. Take all practical measures to ensure that the building or facility is evacuated.	*The individual who first notices or receives word of the explosion should contact the GM immediately by whatever means of communication are available.* *Notification phone numbers can be obtained from the Organization Contact List in Appendix D, Table D-2 as well as from Section 6.1DSRSD Chain of Command of the Emergency Response Plan, (ERP).*
Initiation and Notification:	D. In cases where an adversary calls a DSRSD employee in advance that employee should complete the **Bomb Threat Checklist** Appendix G, Pages G-14 to G-16 or **Phone Threat Report Form** Appendix G, Pages G-6 to G-7. E. Initiate partial or full ERP activation. F. Initiate partial or full activation of the Emergency Operations Center (EOC)	*The **Bomb Threat Checklist** and the **Phone Threat Report Form** contain questions that should be asked the caller if possible to help determine the specifics of the threat including the location of the explosive device, type of device, time of detonation, and reason for the attack.* *The GM will decide whether to*

AP 2 - Structural Damage from Explosive Device		
	Emergency Operations Center (EOC). G. Engage other organization as needed (Law Enforcement, Fire Protection, FBI). H. Perform internal and external notifications according to ERP.	*initiate the ERP on a partial or full basis. The GM will also decide when and to what extent to activate the EOC.*
Equipment Identified:	**Equipment** **Location**	*This equipment is available to assist in the execution of this AP.*
Specific Activities:		
I. Assess the Problem	1. Deploy a Damage Assessment Team(s) (DAT) • Perform a thorough assessment of the structural damage caused by the explosion. • Determine how explosion is effecting system operations. 2. Check and monitor all other water system functions and facilities to ensure that the rest of the system is operating normally. (The initial explosion could be a diversion to a larger event, or it could be the first in a series of similar attacks.) 3. If the damage appears to be intentional, treat as a crime scene. Consult with local police, state police, and the FBI on evidence preservation. Also see **Maintaining Crime Scene Integrity** Form, Appendix G, Page G-5, ERP. 4. Isolate damaged facility from rest of water system, and take measures to bypass the damaged area if possible. 5. Inform local police, state police, and the FBI of potential hazardous materials.	*The DAT will work in conjunction with local/state law enforcement in terms of incident command and control.* ***UNDER NO CIRCUMSTANCES WILL THE DAT TEAM ENTER THE AREA CONTAINING THE EXPLOSIVE DEVICE UNTIL AFTER THE LOCAL LAW ENFORCEMENT EXPLOSION SPECIALISTS (BOMB SQUAD) HAS DETERMINED THAT THE AREA IS SAFE.***
II. Isolate and Fix the Problem	6. Physically secure water system facilities and implement heightened security procedures throughout the system. 7. Based on extent of damage, consider alternate	

AP 2 - Structural Damage from Explosive Device		
	(interim) treatment schemes. 8. Issue public notification, "Boil Water", "Do not Drink", or "Do not Use" orders and other Press Releases as appropriate. See Appendix F for **Press Release Forms**. 9. Request assistance from outside contractors or other water utilities if needed to help repair the damage.	
III. Monitoring	10. Perform sampling and monitoring activities and analysis to determine if the explosion has rendered the water supply unsafe for customers. 11. Perform a system pressure evaluation to determine how the explosion has affected customers and fire water capability in each pressure zone.	
IV. Recovery and Return to Safety	12. Repair damage to critical equipment and facilities as soon as possible. 13. Determine and mitigate effects on other system components. For example, replace water storage capacity if it was diminished during repairs. 14. Clean and disinfect system components as necessary. 15. Resume normal operations. 16. Assess need for additional protection/security measures.	*The GM will inspect the repairs and will give the OK to resume normal operation of the water system* *The GM will evaluate a heightened security posture. As a result, security will be increased or decreased as necessary according to the perceived threat.*
V. Report of Findings	17. File incident reports.	*The Utility GM should file an internal report for the Utility's files, and also provide information as requested to Local Law Enforcement and other outside agencies.*
VI. AP-2 Revision Dates		

This page has been intentionally left blank.

AP4 – SCADA Security		
AP Summary:	This Action Plan applies to a cyber attack on the DSRSD FOD SCADA system when the cyber intruder is: • Conducting DoS (Denial of Service) attack • Initiating SCADA command spoofing attack • Attempting to take the SCADA system down • Attempting to take control of or is in control of the system	
Initiation and Notification:	Notify immediately upon discovery of an attack: • Electrical Services Supervisor (Maurice Atendido) • Operations Manager (Dan Gallagher) • FOD Supervisor (Jim Dryden)	*The individual that first notices or receives word of an attack should contact the Electrical Services Supervisor, the Operations Manager and FOD Supervisor immediately by whatever means of communication may be available.* *Notification phone numbers can be obtained from the Organization Contact List in the Appendices as well as from Section XX of the ERP.* *In all likelihood the Electrical Services Supervisor will have to execute this action plan, but Lino Lantin or Roger Li from the Electrical Division and/or the District IT staff could probably execute the action plan if the Electrical Services Supervisor is unavailable. (In the future, the Instrumentation Technicians are supposed to be able to assist and "back-up" the Electrical Services Supervisor, but much training of the District IT staff and Instruments Technicians would be required to execute certain portions of this action plan.)*
Support Equipment	<u>Equipment</u> - Operations Control Systems Specialist Laptop PC - Spare parts (computers, controllers, telemetry communication equipment) - System back-ups, original software <u>Location</u> - With the Operations Control Systems Specialist - WWTP SCADA store room, FOD SCADA Room, equipment already in use throughout the system - With the Operations Control Systems Specialist & fire proof storage	*This equipment is available to assist in the execution of this action plan.*

AP4 - SCADA Security		
Specific Activities:		
I. Assess the Problem	An attack on SCADA system may be manifested in several different manners and may be quite difficult to initially determine the specific mode of attack or objective of the SCADA threat. The most likely indicators of a cyber attack would be: • SCADA is not controlling one or more facilities correctly (indicated by SCADA alarming, discrepancies between physical rounds and SCADA readings, etc.) • Complaints from customers (such as low water pressure; odor, taste & appearance, etc.) • Unacceptable Water Quality test results (high/low chlorine residuals, high/low fluoride residuals, presences of other contaminants, etc.) • Slow SCADA system response and/or inability to access the SCADA system (both locally and/or remotely)	*A Denial of Service attack is the most likely cyber attack to occur and/or be successful against the FOD SCADA system; due to the isolated nature of the FOD SCADA system (the only remote connection to the FOD SCADA system is through a Terminal Server) and the remote access security (it takes two sets of usernames and passwords to gain access to the SCADA system remotely). The telemetry communications is most vulnerable to, is a Denial of Service attacked – which could be affectively jammed, denying real-time data and potentially causing temporary water storages and/or overflows. Manual operation of the Water System is possible to migrate the affects of any Denial of Service attack.* *Command spoofing is highly unlikely to be successful, based upon the detailed knowledge of the proprietary communications protocol required command spoof. Again, manual operation of the Water System is possible to migrate the affects of any command spoofing attack.* *Physical security is the best defense against any attempt to shutdown the FOD SCADA system. The critical telemetry facilities are the most vulnerable targets for successfully, temporarily taking down the FOD SCADA system, but again operation of the manual Water System is possible to migrate the affects of any system shutdown attack. The modular design of the SCADA system allows common spare parts so any physical damage could be minimized by re-allocating lower priority facilities/ equipment if all spare parts were exhausted.* *The isolated nature of FOD SCADA system described above makes a take-over of the FOD SCADA system very unlikely and could be quickly defeated by serving the Terminal Services connection and/or going to manual operation of the Water System.*

AP4 – SCADA Security		
II. Isolate the Problem	1. Restrict physical access to the area.	*Restricting access helps to preserve fingerprints for later prosecution (if physical access to systems is involved)*
	2. Physically unplug any phone lines that could dial in to the attacked computer.	*These steps isolate the SCADA system from the outside world where the cyber attack is originating.*
	3. Unplug the computer from the network. 4. Determine if the SCADA system needs to be isolated from process operations and taken completely off line.	*The SCADA system itself may be malfunctioning as a result of the attacks with equipment not operating as originally intended.*
	5. Photograph the scene, including connections to any peripherals.	*Useful for later reference if the machine needs to be disassembled for examination.*
	6. IF the computer is off, DO NOT turn it on (preferred method is to jumper system disk drive(s) as read only, and perform a post-mortem on a separate computer using suitable tools.)	*Merely turning on a Windows computer changes time stamps and other important evidence, for example.*
	7. IF the computer is on, DO NOT reboot it.	*Rebooting your computer may launch viruses or time bombs.*
	8. Avoid accessing any files on the compromised machine.	*Access timestamps may be altered.*
	9. Increase sampling throughout system – consider whether to isolate sections of the system.	*Manual sampling may be necessary if computerized process are not functioning properly.* *Contamination may pass through the system unnoticed if an insufficient number of sampling points are used or if sampling points and mis-specified.*
	10. Preserve latest full battery background test at baseline.	*A baseline analysis is important for determining if changes of an unknown nature are made to the water supply*
	11. Check for NIPC water sector warnings (*http://www.NIPC.gov*)	*The NIPC web-site may contain additional protective actions to consider.*

AP4 – SCADA Security		
III. Preserve the Evidence	A Computer Forensics Specialists will be utilized to preserve the necessary computer data for law enforcement.	*The goal is for proper forensics to be performed on the logs and computer files such that a determination as to whether a criminal offense occurred and whom committed the offense. Additionally, the evidence needs to be preserved in a manner that will support prosecution (i.e. - that it cannot be claimed that these logs were tampered or altered and prosecution can therefore take place)..*
IV. Fix the Problems/ Damage caused by the Incident	Only personnel familiar with configuring and maintaining the SCADA system should attempt to restore the FOD SCADA system to normal operation. The qualified personnel have knowledge to restore the FOD SCADA system to normal operation with resources available (system documentation, system back-ups, iGlobalcare support, outside SCADA vendors, etc.)	*The SCADA system documentation, system back-ups and the iGlobalCare Support contract will be the most helpful items to restoring the FOD SCADA System to normal operation*
V. Conduct a "Lessons Learned" Session and Implement any identified corrective measures	1. Conduct a "Lessons Learned Session" 2. Develop a plan for implementing any identified corrective measures 3. Implement the corrective measures 4. Test the previous security breach to ensure the vulnerability is corrected	*Simply returning the system to operation may be insufficient and invite future attacks.* *Ensures attacker cannot use same method to compromise SCADA system.*
VI. AP-4 Revision Dates		

AP 7 – Power Outage

AP Summary:	This Action Plan applies to events that result in power outages. Note that this Action Plan may need to be implemented in conjunction with other Action Plans (for example, severe weather) as necessary.	
Initiation and Notification:	Initiate this AP upon a loss of offsite power. Notify: • GM or designee • Operations Manager • Field Operations Supervisor • Electrical Supervisor • Mechanical Supervisor Others as appropriate, examples include: • Fuel supplier (back up generator) • Critical Care Customers • Large Water Users	*Notify the GM by whatever means of communication may be available.* *Notification phone numbers can be obtained from the Organization Contact List in Appendix D, Table D-2 as well as from Section 6.1DSRSD Chain of Command of the Emergency Response Plan, (ERP).*
Equipment Identified:	Equipment • Mobile battery-powered radios • Mobile/cellular phones • Flashlights • Spare batteries • Accessory requirements (cables for generators, transformers, load banks, bus bars, distribution panels, feeder panels, fuses, outlets, load centers, etc) • Emergency kits	*Radios should have access to a frequency compatible with the local fire dept, sheriff, public health officials, other government departments, utilities, services, or consultants.* *Note: Cell phones may not be available during power outages.*
Specific Activities:		
I. Assess the Problem	1. Call PG&E – request information on the estimated down time. 2. IF backup generation is available, **THEN** assess the need for additional fuel for extended periods. 3. Assess ability for HVAC or alternate to provide proper temperatures for SCADA, computer, and control systems.	*Complete assessment as quickly as possible.*

AP 7 – Power Outage		
	4. Estimate potable water requirements under the emergency condition and determine if the utility can still meet requirements. 5. **IF** telephone is also down, **THEN** SCADA communications may be blocked. 6. Loss of power could affect utility access gates, CCTV, intrusion alarms and other remote monitoring abilities. Loss of power may be a diversionary tactic for other terrorist activity. Be alert.	
II. Isolate and Fix the Problem	7. Turn off unnecessary electrical equipment. 8. Start back up generators as necessary for key components: Note: Uninterruptible Power Supply (UPS) for SCADA and computers, battery back-up for Remote Terminal Unit (RTU) may only supply power for a few hours.	*This can prevent injuries and damage from unexpected equipment startups, power surges to the equipment and possible fires. If power goes out, an Uninterruptible Power Supply (UPS) provides battery power at a constant rate for several minutes, allowing you to safely turn off equipment with minimal risk or loss.*
II. Isolate and Fix the Problem	9. Increase disinfectant residual as a precaution to potential contamination. 10. **IF** not able to meet community requirements for water **THEN** arrange for water to be supplied by another source. See Mutual Aid Agreements Section 2.1.2; Interconnects and Agreements with Other Utilities Section 3.4.2 ; and Water Sources for Short-term Outages, Section 3.4.3 of this ERP. Notify priority customers. 11. Notify users of interruption of service if backup pump(s) is/are not capable of maintaining supply. 12. Issue "Boil Water", "Do not Drink", or "Do not Use" orders and Press Releases as appropriate. See Appendix F for **Press Release Forms and Section 6.0 Communications Procedures.** 13. Initiate back up plan for retrieval of current information from outside sources.	*This is an analysis of all available sources of water, not just those used under conditions of normal operation. These sources might include both new intakes or wells, public or private ponds, reservoirs, swimming pools, interconnections with other water utilities, water stored within building water systems, water provided in bottles or tank trucks from outside sources of potable water, local dairies or bottling plants, etc.* *Since computers may be down, access to Water ISAC, police, government, etc. could be compromised.*

AP 7 – Power Outage		
II. Isolate and Fix the Problem	14. Consider initiating back-up portable pumping and generating capability to serve areas with limited storage, critical wastewater collection and treatment operations.	
III. Monitoring	15. **IF** damage to equipment occurs, **THEN** contact vendor/mutual aid companies to replace/repair damaged equipment. 16. Monitor the status of the backup power supply and regularly test whether battery levels are adequate and the backup generators are functional.	*Ask your vendors about specific limitations of your equipment. Find out how long it would take to repair or replace damaged equipment.*
IV. Recovery and Return to Safety	17. Conduct disinfection, flushing, and bacteriological sampling after repairs of equipment lost. 18. Fire and potable water piping should be checked for leaks from damage after the heat has been restored to the facility and water turned back on. 19. Notify public/customers when it is safe to use the drinking water again.	
V. Report of Findings	20. All the components of the incident should be correlated and established in writing. This would include how the response was managed and suggestions to improve the facility / community response in the future. The report should incorporate all relevant data from the incident and suggested changes in the emergency response plans and procedures. 21. Suggestions from the report should be submitted to the governing board/individuals for evaluation and actions to be taken.	*To learn from the incident and reduce the likelihood of future such events, a Report of Findings should be provided to the decision makers for the Utility so consideration can be given for changes in facility structure, security, procedures or personnel.*
VI. AP-7 Revision Dates		

This page has been intentionally left blank.

AP 8 – Natural Event (Earthquake)		
AP Summary:	This Action Plan applies to earthquakes. In general, these events occur without any lead times, making it impossible to take proactive measures. Response and recovery can be time consuming during such events, and they can involve loss of electrical power supply, damage of structures and equipment, disruptions of service, and injuries to utility personnel.	
Initiation and Notification:	Earthquakes usually occur without any type of warning. Due to the suddenness of these events, all personnel should attempt to find immediate shelter. This may include: • Getting under a desk or heavy table. • Standing flat against an interior wall. **Note: Do not seek cover under laboratory tables or benches as chemicals could spill and harm personnel.** After an earthquake has stopped, initiate this earthquake AP.	*Notification phone numbers can be obtained from the Organization Contact List in Appendix D, Table D-2 as well as from Section 6.1DSRSD Chain of Command of the Emergency Response Plan, (ERP).*
Equipment Identified:	Equipment Location	
Specific Activities:		
I. Assess the Problem	In general, the GM or designee will organize an assessment team to undertake the following activities: • Inspect all structures for obvious cracks and damage. • Assess condition of all electrical power feeds and switchgear. • If SCADA is working, immediately review system for all types of malfunctions, including telemetry, pressure in the distribution system, and operation of pumps and other equipment. • If buildings have any sign of damage, such as cracked walls, broken windows, downed power lines, do not enter, but wait for trained personnel.	*Be prepared for aftershocks. Although smaller than the main shock, aftershocks cause additional damage and may bring weakened structures down. Aftershocks can occur in the first hours, days, weeks, or even months after the quake. Follow the same*

AP 8 – Natural Event (Earthquake)		
	• If buildings appear safe, cautiously inspect condition of interiors for damaged equipment, leaks, chemical spills, etc. • Communicate all findings to Emergency Operations Center (EOC) or GM, as appropriate. • Account for all on-duty staff.	*procedures as for earthquakes.* *See AP 7 for specific power loss procedures.*
II. Isolate and Fix the Problem	If buildings and/or structures appear safe, cautiously assess severity of damage and impact on processes. Use appropriate Personal Protective Equipment (PPE) where possibility of hazard exposure exists. • Inspect chemical feed systems for integrity • Remediate small chemical spills with appropriate spill materials • Inspect condition of process piping and structures for damage, equipment condition, leaks, etc. • Modify process operations as appropriate to minimize hazards and maintain continuity of operations. • Prepare for aftershocks.	
III. Monitoring	At all times, personnel should observe the following general steps: • Stay calm and await instructions from supervisory or management personnel. • Keep away from overturned fixtures, windows, filing cabinets, and electrical power. • Provide assistance and/or call for medical help for injured employees as needed. • If major structural damage has occurred, order a complete evacuation. Structures shall be inspected and evaluated for integrity by trained personnel prior to reentry. • Wear minimal PPE including long pants, a long-sleeved shirt, sturdy shoes, and work gloves. • Look for and extinguish small fires. Eliminate fire hazards. • Monitor commercial radio for instructions. (KCBS, KGO, etc) • Expect aftershocks. • Use the telephone only to report life-threatening emergencies.	

AP 8 – Natural Event (Earthquake)		
IV. Recovery And Return to Safety	General earthquake procedures after an earthquake are as follows: 1. Activate Emergency Operations Center (EOC). 2. Contact emergency assistance as necessary to respond to injuries of staff. (911) 3. The GM or PIO shall notify customers, media, and state and local authorities if service is disrupted or if significant demand management is necessary. 4. Establish Damage Assessment Teams to inspect facilities for structural damage, including: buildings, storage tanks, pipelines, and process equipment. Consider the use of an outside engineering consultant. 5. Prioritize and repair water main leaks. 6. Contact neighboring purveyors for mutual aid arrangements, and open connections as needed. 7. Respond to side effects (loss of power, fire chemical spills, etc.)	
V. Report of Findings	Assemble relevant personnel to review effectiveness of action plan and reinforce lessons learned.	
VI. AP-8D Revision Dates		

This page has been intentionally left blank.

AP 9 – Water Supply Interruption		
AP Summary:	This action plan applies to water supply interruptions. These events will vary in scale from compromised incremental supply volumes to complete, catastrophic loss of water supply. The ability for a utility to successfully respond to a catastrophic water supply interruption will be highly correlated to the existence of interconnections and alternative sources of supply.	
Initiation and Notification:	Catastrophic water supply interruptions will generally be identified by other events, such as physical equipment damage, severe weather or others, which are likely to have a specific direct action plan. Incremental interruptions due to longer-term events such as drought or acute loss of one source, will lead to a prescribed series of contingency measures, as outlined below.	*It is recognized that many utilities will already have an action plan in place to address this event.* *Notification phone numbers can be obtained from the Organization Contact List in Appendix D, Table D-2 as well as from Section 6.1DSRSD Chain of Command of the Emergency Response Plan, (ERP).*
Equipment Identified:	**Equipment** **Location**	
Specific Activities:		
I. Assess the Problem	There are a number of potential levels of severity involved in a water supply interruption. A series of stages of action corresponding to increasing impacts on water are: • Normal Conditions • Water Alert • Water Warning • Water Crisis • Water Emergency	
II. Isolate and Fix the Problem	Each stage has specific customized definitions, in terms of percent of Water Supply reduction, with appropriate actions or restrictions at each stage. Utilities will have a series of escalating penalties for successive violations of restrictions. These stages are: **Normal Conditions** - Normal conditions apply. Water is available; but in arid environments there are specific watering days for various addresses or penalties for excess watering.	

AP 9 – Water Supply Interruption

Water Alert -- A 5% or greater reduction in water usage is to meet the immediate needs of customers. Voluntary conservation encouraged. The water shortage situation is explained to the public and voluntary water conservation is requested (see standard press releases). DSRSD maintains an ongoing public information campaign consisting of distribution of literature, speaking engagements, bill inserts, and conversation messages printed in local newspapers.

Water Warning -- A 15% or greater reduction in water usage is to meet the immediate needs of customers. Water supply shortage is moderate. The utility aggressively continues its public information and education programs. Consumers are asked for a 15 percent or greater voluntary or mandatory water use reduction. Additional landscape irrigation restrictions may be implemented. Businesses may be asked not to serve water in restaurants unless requested.

Water Crisis – A 30% or greater reduction in water usage is to meet the immediate needs of customers. Water supply shortage is severe. Additional requirements may include:

- Dramatic landscape irrigation restrictions; Restrictions on use of potable water to fill or refill new swimming pools, artificial lakes, ponds, or streams until the water crisis is declared over;
- Prohibition of water use for ornamental ponds and fountains;
- Restrictions on washing of automobiles and equipment (such as requiring that it shall be done on the lawn or at a commercial establishment that uses recycled or reclaimed water);
- Restriction of flushing of sewers or fire hydrants to cases of emergency and essential operations, and;
- Introduction of a permanent water meter on existing non-metered services and/or flow restrictors on existing metered services at customer's expense upon receipt of the second water violation.

AP 9 – Water Supply Interruption		
	Water Emergency -- A 50% or greater reduction in water usage is to meet the immediate needs of customers. Water shortage is critical. Additional requirements may include: • Disallowing all landscape irrigation; • Disallowing potable water use for construction purposes such as dust control, compaction, or trench jetting. • Large industrial users may be required to reduce or cease all water use. In addition to these incremental stages, the Utility should prepare for a catastrophic interruption of water supplies. A catastrophic event that constitutes a proclamation of a water shortage would be any event, either natural or manmade, that causes a severe water supply interruption, synonymous with or with greater severity than the "Water Warning" water supply shortage condition outlined above.	
III. Monitoring	Communication of water supply interruption stages should be handled according to the identified public notification procedures. Press releases should also be handled according to the identified utility procedures.	*See ERP Section 6.0.* *See ERP Appendix F for Press Releases.*
IV. Recovery and Return to Safety	Alternative water supply options have been identified in the ERP. In the event of a catastrophic, immediate need, it is likely these will be utilized. This includes information on local interconnections with neighboring sources, area water haulers, temporary storage options, etc. If there have been lines with no water or negative pressures, a precautionary boil order should be issued until line tests on two consecutive days show the lines to be safe. Fluoride residuals should be increased temporarily. The water system may have to valve off portions of the distribution system until above ground storage tanks are refilled. Valved off areas have the potential for external contamination to enter the system through leaking joints or cracked pipe. Before placing a valved off area back in service, the system should issue a precautionary boil order, increase the Fluoride residual throughout the	*See ERP Alternative Water Sources, Section 3.1.3.2 and 3.1.3.3.* *Appendix F, Press Releases.* *See boil order release, Appendix F* *Appendix F, Press Releases.*

AP 9 – Water Supply Interruption		
	system and obtain safe bacteriological samples from representative areas of the system on two consecutive days. The precautionary boil order may be lifted once the required safe samples are obtained. The boil order may only be lifted with the approval of the District Engineer. The system should be repressurized slowly to avoid water hammer and the potential for damage to the lines. Air should be bled from lines as they refill since entrapped air can impede flows and may cause line damage.	
V. Report of Findings	In addition to completing the appropriate filings with local authorities and agencies, DSRSD should assemble the relevant personnel to review the effectiveness of the action plan and reinforce lessons learned in the process.	
VI. AP-9 Revision Dates		